



DEPARTMENT OF THE NAVY
SECRETARY OF THE NAVY COUNCIL OF REVIEW BOARDS
720 KENNON STREET SE STE 309
WASHINGTON NAVY YARD DC 20374-5023

IN REPLY REFER TO

5200
CORB: 000
19 Apr 12

SECNAVCORB POLICY LETTER 2012-4

From: Director, Secretary of the Navy Council of Review Boards

Subj: PRIVACY ACT/PERSONAL IDENTIFIABLE INFORMATION GUIDANCE (PII)/
PROTECTION OF PROTECTED PERSONAL INFORMATION (PPI)

Ref: (a) SECNAVINST 5211.5E

Encl: (1) Best Practices Protocol for Printed and Electronic Media

1. This policy letter cancels SECNAVCORB Policy Letters 4-2006 and 2008-7 and reissues guidance contained therein.
2. The Departments of Defense and Navy are concerned with safeguarding Personally Identifiable Information (PII) to preclude the potential for identity theft. The purpose of this letter is to address the Secretary of the Navy Council of Review Boards' (SECNAVCORB) "best business" practices for ensuring PII is not compromised. These business practices are effective immediately.
3. PPI is defined by reference (a) as "Any information or characteristics that may be used to distinguish or trace an individual's identity, such as their name, social security number, or biometric records." PPI includes not only the subject of files maintained by the individual Boards, but also information pertaining to SECNAVCORB employees. Only personnel designated in writing by their respective Board President, or the Director in cases involving Front Office personnel, are authorized to take home official files and or documents containing PPI. This does not include emergency recall rosters needed to contact employees outside of normal working hours or to execute SECNAVCORB's Continuity of Operations Plan. This policy is designed to ensure maximum protection of PPI under the custody of SECNAVCORB as required by reference (a). Copies of authorizing letters are to be provided to the Privacy Act Manager (SECNAVCORB Counsel).
4. All SECNAVCORB employees (military and civilian) must ensure PII under SECNAVCORB control (case files, medical records, and other personal information of service members or employees) such as social security numbers, dates of birth, residential addresses, and telephone numbers, etc. (in electronic or paper format) are not accessed by or provided to unauthorized individuals. To this end, all personnel will implement the businesses practices in enclosure (1) and ensure transmittal of PII is properly marked "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: Any misuse or unauthorized disclosure may result in civil and/or

Subj: PRIVACY ACT/PERSONAL IDENTIFIABLE INFORMATION GUIDANCE (PII)/
PROTECTION OF PROTECTED PERSONAL INFORMATION (PPI)

criminal penalties.” This disclaimer should be present on all transmissions, including those to authorized recipients of information per the individual board Privacy Act Systems Notices.

5. Should a compromise or loss of PII occur, all affected individuals must be informed as soon as possible, but no later than 10 days after a loss or compromise is discovered. Should a compromise occur, contact SECNAVCORB Legal Counsel immediately. Legal Counsel will then assist in providing the required notification to appropriate individuals.

6. All requests for PII, other than those by authorized routine disclosures per the Privacy Act System notices, should be forwarded to the SECNAVCORB Legal Counsel for processing in accordance with the Freedom of Information Act regulations.



J. A. RIEHL

Copy to:
Board Presidents
SECNAVCORB Counsel
Office Administrator

BEST PRACTICES PROTOCOL FOR PRINTED AND ELECTRONIC MEDIA

1. Review processes and address steps to ensure Personal Identifiable Information (PII) is not compromised.
2. Keep all printed copies of data with PII in properly marked folders.
3. Electronic records and transmissions of PII must be properly marked, stored, and disposed of in accordance with SECNAVINST M-5210.1 Department of the Navy Records Management Manual.
4. Be certain PII is not left open on desktops, file cabinets, photocopy machines, or circulated to individuals who do not have an official need-to-know.
5. Review websites to ensure PII is not posted.
6. Other than when required, minimize or eliminate the use of social security numbers (SSN). If possible, consider truncating the SSN to the last four digits when you need to distinguish individuals.
7. Ensure PII is not stored in your public Outlook folders.
8. Ensure individuals who use laptops are properly trained on the requirement to protect the inadvertent disclosure of PII.
9. Remove all PII from documents prior to posting in web-accessed public reading rooms or circulating to individuals who do not have an official need-to-know.
10. Assess risks for potential compromise of PII in all files, databases, and other formats to ensure proper safeguards are in place to prevent unauthorized disclosures. Review and update safeguards periodically.
11. Ensure all documents containing PII are properly disposed of. Documents should not be disposed of in containers subject to public access. Shredding is the preferred method for disposal of all PII material.
12. Ensure compliance with the safeguards listed for each Privacy Act System notice you are required to maintain.